INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON BLACK HOLE ATTACK IN MULTIPATH ROUTING WIRELESS SENSOR NETWORK

MR. HARSHAL D. WANKHADE, PROF. G.D.GULHANE

1. M.E. Scholar, IBSS College of Engineering, Amravati, Maharashtra, India.
2. Assistant Professor, IBSS College of Engineering, Amravati, Maharashtra, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Wireless sensor networks are vulnerable against various types of external and internal attacks being limited by computation resources, smaller memory capacity, limited battery life, processing power& lack of tamper resistant packaging. The black hole attack is one of the well-known security threats in wireless sensor networks. The intruders utilize the loophole to carry out their malicious behaviours because the route discovery process is necessary and inevitable. In this paper, we analyse the behaviour of wireless network with or without black hole attack with different parameters. Hence from all these result we can conclude that any black hole in the network can degrade the performance of the network.

Keywords: Wireless Sensor Network, routing protocols, End to End delay, Packet Delivery Ratio, black hole attack, NS2.

Corresponding Author: MR. HARSHAL D. WANKHADE

Access Online On:

www.ijpret.com

How to Cite This Article:

Harshal D. Wankhade, IJPRET, 2015; Volume 3 (9): 1781-1789

PAPER-QR CODE

INTRODUCTION

Sensor networks [1][2][3] are highly distributed networks of small, lightweight wireless nodes, installed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or humidity. Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory, sensors, a communication device and a power source inform of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. The applications of sensor networks are endless, limited only by the human imagination [1] [2] [3]. In this paper an overview on various WSN attacks are mentioned with a special mention on balck hole attack. Summery on the counter attacks and possible preventive measures are mentioned. It is to be mentioned that all the attacks are mentioned thoroughly as well as the preventive measures mentioned in thispaper is also not exhaustive. The rest of the paper is as follows: Section 2 gives design issue of WSN followed by section 3 in which various types of routing protocol in WSN are highlighted. In section 4 classification of black hole attack is described followed by in section5 types of black hole attack and counter measure on black holes are discussed. In section 6 open research challenge described and conclusion is stated in section 7.

II. LITERATURE REVIEW

Proposal name	Approach	Assumption	Philosophy
Dynamic system learning using DPRAODV	DPRAODV	Multiple Black Hole	Single non black hole node detects
Cooperative blackhole node detection using DRI and cross checking	AODV	Cooperative blackhole	Single nonblack hole node detects
Blackhole node detection using two different solution	AODV	Multiple blackhole nodes	Single as well multiple nonblack hole detects
Distributed and cooperative mechanism	AODV	Cooperative and distributed	Cooperative detection
Detection of blackhole attack on AODV based mobile ad-hoc using dynamic anomaly detection	AODV	Multiple blackhole nodes	Single non-blackhole node detects
Single blackhole node detection	AODV	Single black hole	Single non-blackhole node detects
Prevention of blackhole attack	Enhancement	Multiple	Multiple non-blackhole

using fidelity table	of AODV	blackhole	detects
Detection of blackhole using DRI and cross checking	Modified version of AODV	Multiple blackhole	Multiple non-blackhole detects

III. ROUTING PROTOCOLS

There are plenty and different routing protocols in WSN and kinds of investigations have been completed in recent decades. In this section, we introduce the famous and popular routing protocols in WSN. Before a mobile node wants to communicate with a destination node, it should broadcast its present status to the neighbours due to the current routing information is unfamiliar. As the information is acquired, the routing protocols is classified into proactive, reactive and hybrid routing.

1. Proactive (table-driven) Routing Protocol

The proactive routing is also called table-driven routing protocol. In this routing protocol, nodes time to time broadcast their routing information to the neighbours. Each node needs to maintain their routing table which not only records the adjacent nodes and reachable nodes but also the number of hops present in the network. In other words, all of the nodes in the network have to evaluate their neighbourhoods as long as the network topology has changed. Therefore, the drawback is that the overhead increases as the network size increases, a large communication overhead within a larger network topology. But, the advantage is that network status can be immediately known if the malicious attacker joins. The most common types of the proactive type are destination sequenced distance vector (DSDV) routing protocol and optimized link state routing (OLSR) protocol.

2. Reactive (on-demand) Routing Protocol

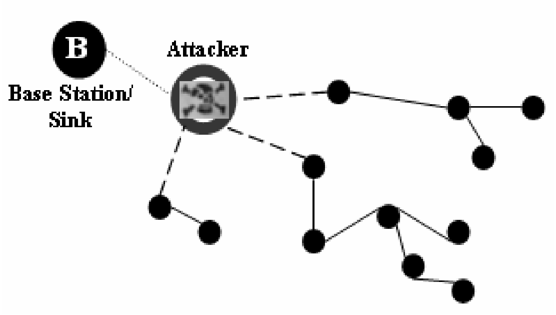
The reactive routing is also named on-demand routing protocol. Unlike the table driven routing, the reactive routing is simply started when nodes desire to transmit data packets. The strong point is that the wasted band width induced from the cyclically broadcast can be minimized. However, this might also be the serious wound when there are any malicious nodes in the network environment. The disadvantage is that passive routing method leads to some packet loss. Most common on-demand routing protocols which is ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) protocol. In AODV, each node only records the next hop information in its routing table but maintains it for sustaining a routing path from source to destination node. If the destination node is unreachable from the source node, the route discovery process will be performed immediately. In the route discovery phase, the source node broadcasts the route request (RREQ) packet first and then all intermediate nodes receive the RREQ packets, but parts of them send the route reply (RREP) packet to the source node if the destination node information is occurred in their routing table. Also, the route maintenance process is started when the network topology has changed or the connection has failed. The source node is observed by a route error (RRER) packet first. Then it uses the present routing information to choose a new routing path or restart the route discovery process for updating the information in routing table. The key idea of dynamic source routing (DSR) is based on source routing. The source routing is the each data packet contains the routing path from source to destination in their packet headers. Unlike AODV which only records the next hop information in the routing table, the mobile sensor nodes in DSR maintain their route cache from source to destination node. From above it is clear that, the routing path can be determined by source node because the routing information is recorded in the route cache at each node. However, the performance of DSR decreases with the mobility of network increases, lower is the packet delivery ratio higher will be the network mobility.

3. Hybrid Routing Protocol

The hybrid routing protocol combines the advantages of proactive routing and reactive routing to overcome the drawbacks of them. Most of hybrid routing protocols are designed as a hierarchical or layered network framework. In the beginning, proactive routing is working to completely gather the unfamiliar routing information, then by using the reactive routing to maintain the routing information when network topology changes. The most commonly use hybrid routing protocols are zone routing protocol (ZRP) and temporally-ordered routing algorithm (TORA).

III. BLACK HOLE ATTACK

Like matter disappears in black hole, in the same way data packets disappear at a node behaving as a black hole node in the MANETs. Black hole attack is a big problem in MANETs in which an intermediate node works as malicious and consumes data before reaching to the destination. Black hole attack works in two phases in first phase, it advertises that it has a fresh route to the destination to deliver data packets with intention to drop data packets. In second phase it drops data packets without forwarding it. In this whenever any intermediate node gets a RREQ it immediately generates a RREP with high destination sequence number and sends it to the initiator. (Source) source stops receiving RREP and starts sending data packet to that node which has sent RREP to the source there are two kind of black hole attack



1. Single Black Hole Attack

In this malicious node individually works as a black bole node. This black hole is easy to detect in comparison with cooperative black hole attack.

2 Collaborative Black Hole Attack

In cooperative black hole attack, there are more than one black hole nodes working in group. It is more complex to detect cooperative black hole attack than single black hole attack.

VI. Analysis & Discussion

In this scenario, all the three routing protocols are evaluated in different number of nodes, keeping other factors fixed and performance evaluated based on the four performance metrics which are Packet Delivery Fraction, End-to-End Delay, Normalized Routing load and Packet Drop Ratio. Table 4 list the simulation parameters applied in the experiments.

Parameter	Value
Number of Nodes	10 to 90 (varying)
Pause Time	2 Seconds
Simulation time	180 seconds
Traffic type	CBR
Data Payload	512 bytes/packet
Mobility Model	Random Way Point Algorithm

Packet Delivery Ratio (PDR): The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

∑ Number of packet receive / ∑ Number of packet send

The greater value of packet delivery ratio means the better performance of the protocol.

End-to-end Delay: the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

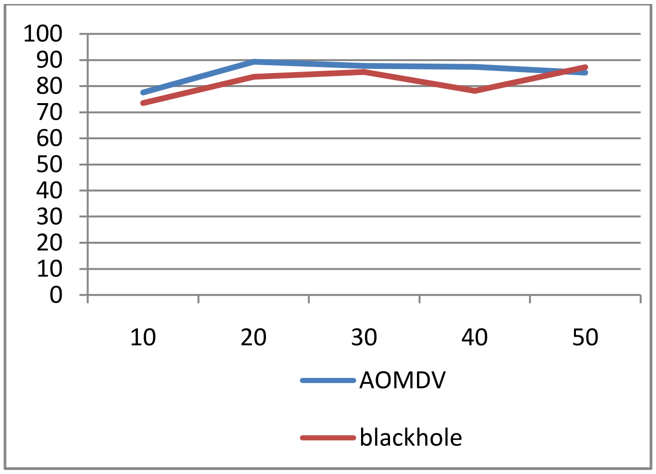
The lower value of end to end delay means the better performance of the protocol.

VI. Results

A. Packet Delivery Fraction

The ratio of the data packets delivered to the destinations to those generated by the constant bit rate (CBR) sources is known as Packet Delivery Fraction (PDF). Fig. 4 shows the PDF of the AOMDV and EENDMRP models for varying number of nodes. The PDF is always high in the EENDMRP model as compared to the AOMDV model. The number of dropped packets in the EENDMRP model is less than that in the AOMDV model. The effective primary path selection mechanism in the EENDMRP model avoids the packet drop over the network.

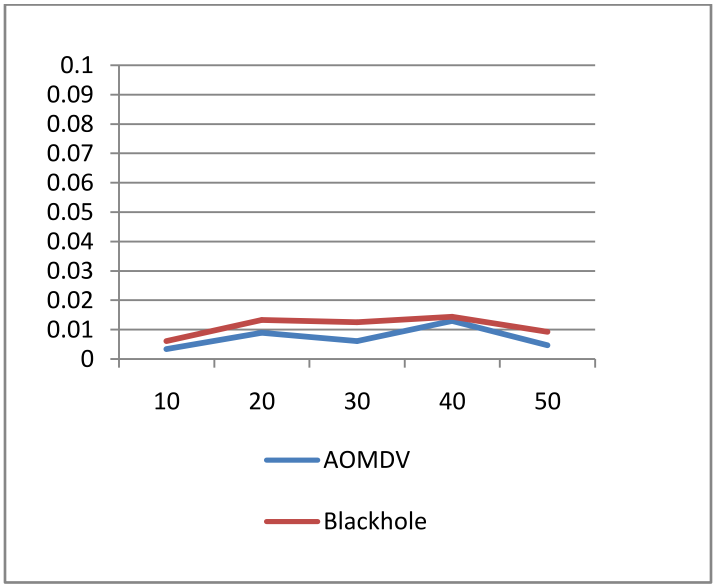
Nodes	PDR	PDR Blackhole
10	77.4613	73.4047
20	89.2206	83.5232
30	87.7165	85.3236
40	87.2835	78.0994
50	85.1413	87.1923



B. Average End-to-End Delay

Average end-to-end delay includes all possible delays due to buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times of data packets. Fig. 5 shows the end-to-end delay incurred in sending the data from the source node to sink node in the AOMDV and EENDMRP models. The end-to-end delay is reduced in the EENDMRP model as compared to the AOMDV model.

Node	E2edelay	E2E Blackhole
10	0.00340795	0.00612434
20	0.00895958	0.0132625
30	0.0060726	0.0125268
40	0.0129921	0.0144254
50	0.00467113	0.00927064



VII. CONCLUSION

After simulation we reach to conclusion that simulation of these two scenarios AODV and AODV with black hole attack, black hole affects the performance of network. The packet delivery ratio decreases and average end to end delay increases after adding black hole attack in AODV protocol. Hence performance of the network under blackhole attack is affected hence we have to develop an effective mechanism which can keep black hole nodes a side and improve the performance under black hole attack. Different preventive techniques are shown in table but these techniques are not work in all condition.

So we need to develop a digital signature based cryptosystem model which can keep nodes in the network authentic and allow safe transmission of data within the network.

VII. REFERENCES

1. M. Tubaishat, S. Madria, (2003) “Sensor Networks: An Overview “, IEEE Potentials, April/May 2003.

2. Jamal N. Al-Karaki& Ahmed E. Kamal, (2004) “Routing Techniques in Sensor Networks: A survey”, IEEE communications, Volume 11, No. 6, Dec. 2004, pp. 6-28.

3. Al-Sakib khan Pathan et.al,(2006) ”Security in wireless sensor networks: Issues and challenges” in feb.20-22,2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048)

4. Ms. Priya Maidamwar, Prof. N. A. Chavhan “A Survey on Routing Techniques for Wireless Sensor Networks”, 2012 National Conference on Innovative Research Trends in Computer Science Egg. & Technology.

5. Ms. Priya Maidamwar, Prof. N. A. Chavhan“ A SURVEY ON SECURITY ISSUES TO DETECT WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK”, International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012.

6. Al-Shurman M, Yoo S-M, Park S (2004) Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42ndAnnual ACM Southeast Regional Conference (ACM-SE’42), Huntsville, Alabama, 2-3 April 2004.

7. Tamilselvan L, Sankaranarayanan V (2007) Prevention of Blackhole Attack in MANET. Paper presented at the 2ndInternational Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

8. Djenouri D, Badache N (2008) Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6.

9. Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009.

10. Raj PN, Swadas PB (2009) DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET. International Journal of Computer Science 2:54–59. doi: abs/0909.2371.

11. Jaisankar N, Saravanan R, Swamy KD (2010) A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26-27 March 2010.

12. Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K (2003) Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.

13. Weera singhe H, Fu H (2007) Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007.